SC402- Introduction to Cryptography
Assignment 3

1. Define a toy hash function $h : (\mathbb{Z}_2)^7 \to (\mathbb{Z}_2)^4$ by the rule $h(x) = xA$ where all operations are modulo 2 and

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

   Find all preimages of $(0, 1, 0, 1)$.

2. If we define a hash function (or compression function) h that will hash an n-bit binary string to an m-bit binary string, we can view h as a function from $\mathbb{Z}_{2^n}$ to $\mathbb{Z}_{2^m}$. It is tempting to define h using integer operations modulo 2^m. We show in this exercise that some simple constructions of this type are insecure and should therefore be avoided.

   (a) Suppose that $n = m > 1$ and $h : \mathbb{Z}_{2^m} \to \mathbb{Z}_{2^m}$ is defined as

   $$h(x) = x^2 + ax + b \mod 2^m.$$

   Prove that it is (usually) easy to solve **Second Preimage** for any $x \in \mathbb{Z}_{2^m}$ without having to solve a quadratic equation.

   HINT Show that it is possible to find a linear function $g(x)$ such that $h(g(x)) = h(x)$ for all x. This solves Second Preimage for any x such that $g(x) \neq x$.

   (b) Suppose that $n > m$ and $h : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^m}$ is defined to be a polynomial of degree d:

   $$h(x) = \sum_{i=0}^{d} a_i x^i \mod 2^m,$$

   where $a_i \in \mathbb{Z}$ for $0 \leq i \leq d$. Prove that it is easy to solve **Second Preimage** for any $x \in \mathbb{Z}_{2_n}$ without having to solve a polynomial equation.

   HINT Make use of the fact that $h(x)$ is defined using reduction modulo 2^m, but the domain of h is $\mathbb{Z}_{2^n}$, where $n > m$.

3. Suppose that $f : \{0,1\}^m \to \{0,1\}^m$ is a preimage resistant bijection. Define $h : \{0,1\}^{2m} \to \{0,1\}^m$ as follows. Given $x \in \{0,1\}^{2m}$, write

   $$x = x' \mid\mid x''$$

   where $x', x'' \in \{0,1\}^m$. Then define

$$h(x) = f(x' \oplus x'').$$

Prove that h is not second preimage resistant.

4. Suppose $h_1 : \{0,1\}^{2m} \to \{0,1\}^m$ is a collision resistant hash function.

   (a) Define $h_1 : \{0,1\}^{4m} \to \{0,1\}^m$ as follows:

      1. Write $x \in \{0,1\}^{4m}$ as $x = x_1 \mid\mid x_2$, where $x_1, x_2 \in \{0,1\}^{2m}$.
      2. Define $h_2(x) = h_1(h_1(x_1) \mid\mid h_1(x_2))$.

      Prove that h_2 is collision resistant (i.e., given a collision for h_2, show how to find a collision for h_1).

   (b) For an integer $i \geq 2$, define a hash function $h_i : \{0,1\}^{2^i m} \to \{0,1\}^m$ recursively from h_{i-1}, as follows:

      1. Write $x \in \{0,1\}^{2^i m}$ as $x = x_1 \mid\mid x_2$, where $x_1, x_2 \in \{0,1\}^{2^{i-1} m}$.
      2. Define $h_i(x) = h_1(h_{i-1}(x_1) \mid\mid h_{i-1}(x_2))$.

      Prove that h_i is collision resistant.